DIR
CYBERSECURITY
INSIGHT
Newsletter

February 2014

ADDRESSING THE EVERCHANGING RISKS FOR THE STATE OF TEXAS

DIR Security Services at a glance

Securing the Human

OCISO continues offering *Securing the Human* end-user training for those Agencies that want to enforce and enhance their Security Awareness Program.

If your organization handles regulated data that needs to comply with Federal and State rules and regulations, you can use this training for compliance.

There are 24 compliance modules such as: FERPA, HIPAA, PCI-DSS, PII, Criminal Justice, Federal Tax and more.

OCISO has assigned a number of seats for your agency. If you haven't setup your training and want to keep your seats, reach out to the OCISO soon. By the end of March all unused licenses will be pulled out and redistribute to other agencies.

Decision Support

IT Leaders, Security and Privacy professionals deal with new projects and emergent technologies every day. To keep up to date on magic quadrants, vendor leaders and technology, DIR offers Gartner research license for your Agency as a valuable resource.

Gartner provides extensive research capabilities, creating a good source for addressing IT issues, with objective and rapid access to IT insights.

Controlled Penetration Testing

Our goal is to find vulnerabilities before the threats find them.

A comprehensive penetration test can be scheduled for your agency every year, followed by remediation verification and quarterly scans to identify vulnerabilities in your network.

If you haven't scheduled yours, you need to contact our office.

For more information on Security services, send an email to DIR Security.

IN THIS ISSUE

Conference Day 1

"**Transforming Cybersecurity Visibility and Capabilities**." Topics will include:

Welcome and OCISO Update
Karen Robinson, CIO, State of Texas
Brian A. Engle, CISO, State of Texas

Keynote
Dr. Andy Ozment, Senior Director for Cybersecurity, White House

Operationalizing the Cyber Security Framework
Michael Brown, Real Admiral , USN (Ret) VP and General Manager, RSA Global Public Sector

Verizon Data Breach Insights
Jay Jacobs, Senior Data Analyst, Verizon's RISK Team, Verizon

Application Security Threat Modeling
Barry Lyons,Senior Cyber Architect, Northrop Grumman

Advanced Threats Disassembled
Chad Holmes, Chief Security Architect, OCTO, FireEye, Inc.
Ben Frazier, Security Engineer, Mandiant

Adapting Incident Response to Meet the Threat and Minimize the Impact of a Breach
Jeff Schilling, Director, Incident Response and Digital Forensics, Dell SecureWorks

ISF REGISTRATION

Information Security Forum Registration

Workshops - Day 2

Register for day 2 @
Workshops day 2

TRACK A

8:30 – 12:00 **Texas Security Framework and Agency Security Plans**
DIR Staff
Hosted by DIR
Audience: Texas State Government ISOs, IRMs, Auditors, Security Staff

1:15 - 3:15 **TAC 202 Preview Session**
Hosted by SISAC Policy Subcommittee
Audience: Texas State Government ISOs, IRMs, Auditors, Security, Legal Staff

TRACK B

8:30 – 10:00 **Security Battleground: Riches, Ruin & Regulation**
Brian Kenyon, McAfee
Hosted by SISAC Privacy Subcommittee
Audience: Texas Public Sector Privacy staff, Legal, IRMs

10:30 – 12:00 **Incident Handling at Employees Retirement System of Texas**
Victoriano Casas, ERS & Bert Hayes, Splunk
Hosted by: DIR Statewide Security Operations
Audience: Texas Public Sector Security Operations Staff

1:15 - 3:15 **Audit and Security Collaboration Workshop (Topic TBA)**
Hosted by ISACA
Audience: Public Sector and ISACA Members

SPOTLIGHT

LANE GREENE

Information Security Officer for West Texas A&M University

Tell us about yourself.

I grew up in a small town in West Texas and attended West Texas A&M obtaining a BBA in Computer Information Systems. I have worked at the University for almost 15 years starting as a student worker and moving my way up to my current position as the Information Security Officer. To relax I will usually catch whatever ballgames are on TV or play the occasional round of golf.

How did you come to the Security field?

The University made the decision to hire a full time ISO and having a good working knowledge of departmental computing needs around the campus, I quickly found myself with new responsibilities. I soon discovered that job fit me well and I haven't looked back.

What do you like best of your job?

I enjoy the hectic pace, and the challenges that security presents. There is never a dull moment and I have to stay on top of everything happening not only in IT but also throughout campus.

West Texas A&M UNIVERSITY™

What other career would you have liked to pursue?

History professor, I love reading history books and watching documentaries. The small details about how people lived hundreds of years ago fascinate me.

Tell us about your most proud accomplishment?

While I can only take a portion of the credit, I'm proud of the information security program that we've been able to architect at West Texas A&M. Building the program and working with campus stakeholders to achieve consensus can sometimes be challenging, but I've often found its one of the most rewarding accomplishments of my career.

People would be surprised to know that you

I have never seen any of the Star Wars movies or most other sci-fi movies. While I think this is perfectly normal most of my co-workers within IT are amazed by this.

INFORMATION SECURITY
WEST TEXAS A&M UNIVERSITY

What is the best advice you have received and that you have used?

My father has always stressed to only focus on what needs your attention at that moment. This is not an easy to do in security when many different systems or issues may need attention all at the same time. But by only focusing on one thing at a time even if I only have a brief moment easy decisions can be made quicker giving me time to move to more to the complex issues.

What would be your advice for a new security professional?

Find someone in the security profession that you can turn to for guidance, even if they are outside of your organization. For the first few months, things are going to be coming at you fast, kind of like drinking out of a firehouse, and having someone who can help you see the underlying issues and associated solutions will be the key to your success.

Cybersecurity Tips by MS-ISAC Multi-State Information Sharing & Analysis Center

MS

As we look ahead toward the cyber threats facing us this year, some key challenges will result from the advancements in technology that are becoming part of our daily lives. Ranging from the Internet of Things to online currencies, devices and systems have never been more interconnected. Before we adopt these new technologies, we need to ensure we understand the security implications, and have appropriate layers of defense in place.

Below are highlights of several of these new advancements and how they may affect us.

The Internet of Things

What is the Internet of Things? Put simply, the Internet enables connectivity from virtually any end-user device or thing. The latest trend is connecting things such as small appliances, refrigerators, personal medical devices, wearable health trackers and many other items.

One of the most common examples of how the Internet of Things impacts our daily lives is the automobile, which has become a sophisticated computer device. Researchers have demonstrated the ability to hack an automobile's systems to control the brakes, steering wheel, and even shut down the engine. Numerous discussion forums focus on the use of vehicle-to-vehicle (or V2V) technology, which will allow vehicles to talk to each other via wireless connectivity.

Bluetooth, which is a standard feature in many automobiles with options to include a personal hotspot, can allow a modern smartphone to connect to the automobile's stereo system to receive continuous Twitter feeds, or a system that may allow a technician to provide assistance in case of emergencies. Researchers have discovered ways to inject malicious codes/programs through CD players or iPod connectors. So theoretically, an infected song on your iPod or CD, when played in your automobile, potentially can spread malicious code from the automobile's entertainment network to other components of the automobile without many restrictions.

In another example of how the Internet of Things can impact us is from a recent news story, which suggested electric teakettles and other small appliance were able to exploit unencrypted WiFi and send data back to foreign servers[1].

Internet-connected devices that are able to process sensitive personal information tend to be high priority targets for cyber criminals. It will become increasingly critical in 2014 to protect these devices from unintended or unauthorized connectivity.

Bitcoins

A Bitcoin is a digital currency stored in a downloadable wallet on a user's personal computer or with an online wallet service provider. Each wallet has a unique identifier that allows users to transfer bitcoins to other users' wallets. Bitcoin is a decentralized, peer-to-peer payment system, currently with no regulatory authority. It is gaining popularity, with mainstream businesses adopting it as an alternative form of payment or investment.

While the long-term use of Bitcoin is uncertain, for at least the near term in 2014, the increasing adoption and publicity will continue to draw the interest of cyber criminals who target Bitcoin users' wallets for theft, or compromise systems to generate bitcoins via malware infection.

Mobile Transaction Risks

Every new smart phone, tablet or other mobile device provides an opportunity for a potential cyber attack. New features such as Near Field Communications (NFC), as well as AirDrop and Passbook for Apple, will continue to expand in 2014, increasing the opportunities for cyber criminals to exploit weaknesses. NFC and AirDrop allow for similarly configured smartphones to communicate with each other by simply touching another smart phone, or being in proximity to another smartphone. This technology is being used for credit card purchases, boarding passes, and file sharing, and will most likely be incorporated into other uses in 2014.

Risks of these technologies could include eavesdropping (through which the cyber criminal can intercept data transmission such as credit card numbers) and transferring viruses or other malware from one NFC/AirDrop-enabled device to another.

Summary

Before adopting any of the myriad new technologies that are rapidly being deployed, it's important to understand the implications and risks. While interconnectivity can yield many benefits, the risk could outweigh the benefit if the devices, systems and technologies are not properly secured.

Gartner Webinar

Detect data Breaches with user activity monitoring.
Tuesday March 11, 2:00 PM

Registration at

[DIR Security Training]

Cybersecurity Online Training

Recorded Insider Threat: Log Analysis & Correlation
Tuesday, February 4, 2014 2:15:00 PM CST - Wednesday, February 4, 2015 3:15:00 PM CST

Preparing for an Intl Advanced Persistent Threat - 8 AM EST
Thursday, February 20, 2014 7:00:00 AM CST - 8:30:00 AM CST

Preparing for an Intl Advanced Persistent Threat - 1 PM EST
Thursday, February 20, 2014 12:00:00 PM CST - 1:30:00 PM CST

Network Fundamentals – Part 1 - 8 am EST
Tuesday, February 25, 2014 7:00:00 AM CST - 8:30:00 AM CST

Network Fundamentals – Part 1 - 1 pm EST
Tuesday, February 25, 2014 12:00:00 PM CST - 1:00:00 PM CST

What your Mobile Device Says About You 8 AM
Thursday, February 27, 2014 7:00:00 AM CST - 8:00:00 AM C

DIR
CYBERSECURITY
INSIGHT
Newsletter

DIRsecurity@dir.texas.gov